Response to Comments on the May 3, 2004 Public Review Version of "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns”

Background

From May 3 through June 2, 2004, the Homeland Security Working Group of the Federal Geographic Data Committee (FGDC) received comments on “Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns” (Federal Geographic Data Committee, 2004a). The public comment period was announced through a Federal Register notice (69 FR 24182). Representatives of the member organizations of the Federal Geographic Data Committee, including members of the Steering Committee (Federal Geographic Data Committee, 2004b) and the Coordination Group (Federal Geographic Data Committee, 2004c), professional organizations, members of several electronic mail lists for geospatial data and libraries also received invitations to provide comments. Several online and print publications carried a notice about the guidelines and the opportunity for public review and comment.

The guidelines were accessed from the FGDC web site through 2,902 visits by 2,154 unique visitors[1] during the public review period. Figure 1 shows the breakdown of the top-level Internet domains of the visits. These statistics do not include persons who received the guidelines from sources other than the FGDC site (for example through an electronic mail message attachment or from another web site).

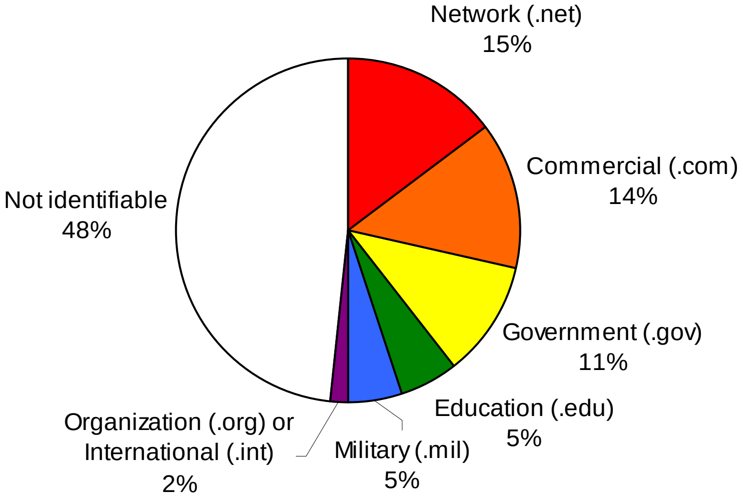

Figure 1. Top-level Internet domains of visits through which the guidelines were accessed during the public review period. Among the addresses in the “not identifiable” category are those that end with “.us”, a style typically used by state and local governments.

[1] A “unique visitor” is an individual who visited the Internet site. The occurrence of a “unique visit” is captured and identified automatically by the site. In the case of guidelines, the “site” was the file that contained the guidelines and instructions to reviewers.

The working group appreciates the interest of the community in the guidelines, and especially the efforts of those who provided comments.

The amended guidelines are being forwarded to the Steering Committee of the FGDC for approval and are available, along with this document, through the working group's home page at http://www.fgdc.gov/fgdc/homeland/index.html.

Overview of Comments

The working group received 46 comments from Federal government (14 comments), commercial (12), local government (7), state government (5), military (3), nonprofit (3), and educational (2) personnel. Some comments reflected the views of organizations or consortia and others reflected views of individuals.

Comments and Responses

All comments were carefully considered. This document provides a summary of the significant comments and responses. Headings identify major themes among the comments. Each heading is followed by one or more general topic(s) from the comments and the response from the working group.

Support of the Guidelines

Comment: Many comments about the guidelines were positive. The majority of reviewers felt that the guidelines offered a logical process to be applied in making their decisions about data dissemination.

Response: Due to the large number of positive comments, changes to the guidelines were carefully made to avoid reducing the value of the guidelines to the majority of reviewers.

Comment: Many comments expressed appreciation for the balance between encouraging access to information and effectively safeguarding information that is truly sensitive. The fact that the guidelines encourage data originators to provide access to information also was appreciated.

Response: These two important principles sometimes compete, and finding a balance between them can be difficult. The working group appreciates the compliments on its efforts to encourage decision makers to find this balance.

Intent and Use of the Guidelines

Comment: The guidelines should carry the weight of regulation and have enforcement actions.

Response: The guidelines were not intended as a regulatory process or as a prescription for implementation. The approach used to develop the guidelines responds to the following conditions:

- Organizations can and do safeguard information that they believe to be sensitive, but do so without considering whether data require safeguarding and what safeguards are authorized and justified.
- Inconsistent decisions among organizations may undermine the effectiveness of any one organization's actions.

- Many types of organizations can and do generate geospatial data and information, including business, academic, non-profit, and government organizations. They operate under a large variety of conditions. For example each level of government, and sometimes an individual organization, can have its own unique set of laws and regulations related to public access to information, specific requirements for distribution of public information, and allowable exemptions to public requests for information with which it must comply. Each also has its own "network" of expertise upon which it must rely in making decisions regarding data access.

It is not practical to provide a highly detailed, in-depth prescription for data safeguarding that would adequately cover all organizations. The guidelines offer a more practical option in which organizations can follow a common procedure voluntarily, integrating it with their circumstances.

Comment: Decisions made using the guidelines are subjective and may be contradictory. Because the use of the guidelines is voluntary, actions among organizations may be contradictory because all organizations will not use them.

Response: The guidelines offer a logical decision-making process that will help organizations to make more uniform decisions. The working group recognizes that use of the guidelines is voluntary and that their use (or lack thereof) may result in inconsistent determinations. Nevertheless, the widespread use of the guidelines will result in much greater consistency and more effective action than at present, because the geospatial data community is now making decisions about safeguarding data with few or no guidelines.

Comment: The existence of the guidelines will encourage organizations to make decisions about the sensitivity of their data. A related comment is that some organizations do not wish to do so.

Response: The lead paragraph of the guidelines states that the majority of data are appropriate for public release, but that a small portion require safeguarding. For organizations that are making decisions about safeguarding sensitive data, the guidelines provide a procedure for identifying geospatial data that need safeguarding and safeguards that are appropriate and authorized.

Comment: The guidelines should require that the appropriate executive management and legal counsel in an organization, instead of information technology and other technical staff, be involved in decisions to apply the guidelines.

Response: The guidelines were modified to reinforce the point that executive management and legal counsel should be key contributors to the decision-making process.

Comment: Evaluating geospatial data using the criteria in the guidelines is a challenging activity. The guidelines should specify instructions on access restrictions for data layers that are sensitive and provide a comprehensive list of potential targets and methods of attack.

Response: The publication "Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information" (Baker and others, 2004) is a good resource for understanding the criteria used in the guidelines for assessing the need to safeguard a set of geospatial data. In addition, the working group plans to provide clear examples of how the guidelines are being implemented by various agencies. As this body of knowledge increases over time, it will provide more specific or "concrete" examples of how to review particular data. It will also help to stimulate dialogue on this topic which should lead to further clarification of important issues.

Comment: The guidelines should treat each data delivery mechanism (for example web service, data set, map) differently.

Response: The items of interest to an adversary are the individual components of *information* contained in the data, not the geospatial data taken as a whole or their delivery method. The guidelines are intended to help agencies institutionalize a logical review process that considers the informational value of their geospatial data.

Recommendation of Additional Federal Review

Comment: The guidelines should receive additional agency and legal reviews at executive levels within the Federal Government before they are issued by the FGDC.

Response: Personnel from the U.S. Office of Management and Budget informally reviewed the guidelines before they were released for public comment. Additional Federal review of the guidelines is anticipated before adoption by the FGDC.

Expansion of Examples to Include Populations

Comment: The guidelines discuss concerns about sensitive information related to facilities that might be attacked, but not about groups of people that might be attacked or at risk. Expand the guidelines to include discussion of attacks against people.

Response: The guidelines only provide procedures to identify sensitive information that could be useful to an adversary in selecting specific target(s) and/or for planning and executing an attack on a potential target. Information about populations must be considered as part of the decision-making process, especially when the population itself is a target or is a key part of an attack scenario. However, housing facilities and sites where large numbers of individuals can, or do, gather are often easy to identify and locate using non-geospatial information, in which case safeguarding geospatial data about these sites is ineffective.

Discussion of Privacy Issues

Comment: Discuss issues of personal privacy in the guidelines.

Response: The important topic of protecting personal privacy is outside the scope of the guidelines.

Instructions for Documenting the Use of the Guidelines in Metadata

Comment: The guidelines instruct originating organizations to provide documentation of the use of guidelines in metadata, but do not describe how to do so.

Response: A new appendix 2 specifies data elements from the "Content Standard for Digital Geospatial Metadata" (Federal Geographic Data Committee, 1998) to be used to document use of the guidelines.

Decisions about the Uniqueness of Data

Comment: What is the threshold for "uniqueness" of information (Step 5)? For example, would the accidental release or publication of sensitive information cause it not to be unique?

Response: The step (Step 5) is provided for an organization to assess the effectiveness of safeguarding geospatial data that have been identified as containing sensitive information and to discourage ineffective actions to safeguard data. If the information thought to be sensitive is available from other sources, an organization's effort to safeguard the data is unlikely to be effective at decreasing vulnerability. This is especially is true for "sensitive" information in geospatial data that also is available in open sources or is readily observable. Accidental releases of information would have to be considered on a case-by-case basis.

Comment: Information that can be gained by observing a feature from a public location should not be included in evaluations of the "uniqueness" of information (Step 5).

Response: If the information can be observed, actions to safeguard that information are unlikely to be effective. The publication "Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information" (Baker and others, 2004) provides more insight on this subject.

Guidelines Implementation

In the invitation for public comments, the working group also invited ideas about steps needed to implement the guidelines. These suggestions are listed for information purposes:

- Training
  - Need to train decision-makers in implementing the guidelines.
  - Provide a list of frequently asked questions (FAQ's), a registry of decisions, and other follow-up information.
  - Develop "best practices" models for implementing the guidelines.
  - Identify sources of expertise that organizations could consult to help make determinations about the sensitivity of information.
- Collaboration and adjudication of disputes
  - Establish or identify a "board" or agency to adjudicate differing interpretations or disputes that arise from the application of the guidelines.
  - Develop a means for organizations to collaborate on decisions and resolve disputes, possibly through the FGDC.
- Organizations' implementations
  - Means of disseminating data should include a capability to inform users about changes in decisions about the sensitivity of the information content of geospatial data. Include the capability to recall from users geospatial data that are identified as having sensitive information content after they are disseminated.

References

Baker, John; Lachman, Beth; Frelinger, David; O'Connell, Kevin; Hou, Alexander; Tseng, Michael; Orletsky, David; and Yost, Charles, 2004, Mapping the risks: assessing the homeland security implications of publicly available geospatial information: Santa

Monica, Ca., RAND Corporation, 195 p. (Also available through the RAND Corporation web site at http://www.rand.org/publications/MG/MG142/) (Accessed August 12, 2004)

Federal Geographic Data Committee, 1998, Content standard for digital geospatial metadata (FGDC-STD-001-1998): Reston, Va, Federal Geographic Data Committee, 78 p. (Also available through the Federal Geographic Data Committee web site at http://www.fgdc.gov/metadata/contstan.html) (Accessed August 12, 2004)

Federal Geographic Data Committee, Homeland Security Working Group, 2004a, Guidelines for providing appropriate access to geospatial data in response to security concerns (public review version): Washington, May 3, 2004, 13 p. Available from the Federal Geographic Data Committee web site at http://www.fgdc.gov/fgdc/homeland/FGDC_access_guidelines.pdf. (Accessed August 26, 2004)

Federal Geographic Data Committee, 2004b, The FGDC steering committee: Federal Geographic Data Committee web site at http://www.fgdc.gov/fgdc/fgdc_org.html. (Accessed August 26, 2004)

Federal Geographic Data Committee, 2004c, The FGDC coordination group: Federal Geographic Data Committee web site at http://www.fgdc.gov/fgdc/fgdccg_org.html. (Accessed August 26, 2004)

Request for public comments on guidelines for providing appropriate access to geospatial data in response to security concerns, Federal Register 69:85 (3 May 2004), p. 24182.

The following is the recommended bibliographic citation for this document:

> Federal Geographic Data Committee. Homeland Security Working Group. “Response to Comments on the May 3, 2004 Public Review Version of ‘Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns’”. Washington: September 7, 2004, 6 p. Available through Federal Geographic Data Committee web site at http://www.fgdc.gov/fgdc/homeland/index.html.